Dot cons: Exploitation and Fraud on the Internet — Part 2

Mark Griffiths

In a previous article for *The Criminal Lawyer* (No.l32, May 2003: Griffiths), it was highlighted that the Internet has become the new medium for scam artists. Fraudsters who used to use telemarketing, infomercials, print media, and the mail to attract consumers to their products, services, or investment schemes, are now using cyberspace to promote familiar schemes such as bogus stock offerings, high-tech investment opportunities, and credit-repair services. A few years ago, there was a US law enforcement effort that targeted the top 10 Internet scams. These were culled from Consumer Sentinel, a database of more than 285,000 consumer complaints established and maintained by the Federal Trade Commission. Since then, the FTC and two UK organizations (Department of Trade and Industry, Office of Fair Trading) now share information and have a co-ordination agreement to combat cross-border fraud.

Perhaps the most familiar menace is spam (ie, unsolicited e-mail) offering instant access to any number of commercial services, "one-time-only" discounts on products, or "once-in-a-lifetime" opportunities to get rich quick. Most spam e-mails include within the body text a clickable link that holds the promise of removal from the mailing list. However, following those instructions will often result in the exact opposite. Clicks on 'unsubscribe' links are used by spammers as an electronic signal that the e-mail address is accurate and active, and ready to be sold to other spammers.

Another potential fraudulent activity is the use of Internet pop-ups - shrunken browser windows that often appear when web surfing. Often these are straightforward adverts -

harmless (albeit irritating) commercials that can be closed easily. However, many have more malicious intent. One common example is a pop-up window warning that, unbeknownst to the individual, the computer is transmitting their personal information to all and sundry. The remainder of this article briefly overviews other scams and fraudulent activity that were not covered in the first article.

Pyramid Scheme Scams

Pyramid schemes are illegal under the Fair Trading Act but are highly prevalent on the Internet. These scams promise money or valuables in exchange for soliciting new members. Pyramid schemes are only successful if new members join the group. If no new members join, the pyramid falls, and those at the bottom lose their initial investment. These schemes are typically promoted as games, buying clubs, motivational companies, mail order opportunities, or investment organizations. Pyramid schemes come in many guises but usually have distinguishing characteristics. Firstly, they will promise a financial return based on the number of people you are able to recruit to enter the scheme. Secondly, any money made will primarily depend on the continued introduction of new members to the scheme and not the sale of a particular product or service.

Internet Mall Scams

These scams involve internet malls' that comprise web page collections offering special buying opportunities to consumers. They make a profit by leasing web pages and selling recruitment licenses. For a large up-front fee, individuals can obtain a license to solicit new members and get a percentage of the membership fees they collect. However, these memberships are virtually impossible to sell, so consumers usually end up losing their investment. This type of recruitment plan is also used to market other "business opportunities" (see next section).

Business Opportunity Scams

These scams are presented as legitimate investments. One of the most popular is the "prime bank scheme" scam. Here, promoters of dubious investment schemes claim that there is a secret international market in "prime bank" instruments. They guarantee investors high returns by trading these instruments. In reality, there is no such market. Typically, an individual is invited to put money into a trust account, backed by a guarantee (often fake) from "a top world or European bank". The individual is told that their money will be leveraged to buy prime bank instruments that can be traded for very high returns. In reality, the money goes offshore never to return.

Employment Scheme Scams

From time to time advertisements appear on the Internet offering an incredible employment opportunity offering "the ability to work from home, at your own pace, and still make loads of cash". The most common examples of employment schemes include envelope stuffing, designing computer graphics and e-mail processing. In these cases, individuals are required to buy address lists or software necessary to perform the "work" up front. In more extreme cases, individuals may end up sending money away to a PO Box, or forwarding their credit card details, before they start. Often, the individual will never hear from the company again and the money is lost.

Advanced Fee Scam (aka the 'Nigerian' Scam)

Perhaps the most notorious online scam - and the one with potentially the most serious consequences for unsuspecting victims - is the Nigerian letter scam (also known variously as the advance-fee swindle, the money-transfer hoax, or the 419 fraud). Using e-mail, perpetrators of the fraud adopt a scatter-gun approach. The letters all variations on a theme, usually personally addressed, purports to be from top officials in the Nigerian (or some other) Government who want help in moving millions of dollars from a business deal. They say they only want your bank account number and in return promise to make you a millionaire. However, once an individual is involved, they will require large "advanced fees" for processing in order to "complete the deal". In fact, there is no government official, and no multi-million dollar booty.

Credit Card E-mail Scams

There are many different credit card e-mail scams in operation. In one scam, fraudsters attempt to steal an individual's credit card details by convincing them that it has already happened. A message is sent along the lines:

> "Recently we have received an order made by using your personal credit card information. This order was made online at our official web site on |date]. Our Fraud Department has some suspicions regarding this order and we need you to visit a special Fraud Department page at our web store where you can confirm or decline this transaction by providing us with the correct information."

A link is given which looks like a page within the legitimate web site where the individual completes a form that requests extensive personal information, including credit card numbers and security details. Other similar scams operate with e-mails informing an individual that "We regret to inform you that there was a recent attack by a hacker on your billing or password information". As with the example above, individuals are asked to go to a web site and divulge personal information. Another popular scam involves companies who offer to fix or repair an individual's credit rating for free. However, these companies often charge an up-front fee and do little to improve the credit rating.

Online Auction Scams

In the global marketplace anyone can set up shop selling anything, even if they have nothing to sell. Trading as Calvin Auctions, Chris Chong Kim spent two years selling and reliably delivering small items to countless eBay users, generating lots of praise along the way. Armed with excellent feedback from thousands of consumers, he then posted a plethora of high-value lots - desktop PCs, organizers and notebook computers. Spurred on by Calvin Auctions' good name, many people placed bids on the items, eventually passing on hundreds of thousands of dollars in payment. He then disappeared with all the money leaving the auction winners with nothing.

Disaster-relief Fund Scams

Charity web sites that accept contributions are not new. Unfortunately, **fraudsters** are also getting in on the act and taking advantage of people's generosity online. There have **been** many reports of fraudsters sending out e-mails **asking** for assistance for "emergency relief funds" (such as September 11) and directing recipients to contribute money to the Red Cross through the fraudulent websites. Many of these fraudsters are trying to steal money and credit card numbers. Another type of similar e-mail scam refers recipients to a Web page that, again, contains legitimate lists of resources and links to charitable organizations. However, these sites are full of banner advertisements and links that, when clicked, earn money for the web site's owner.

Invoicing Scams

Another popular scam is when a fraudster attempts to bill an individual for something they did not order (eg, advertising, goods etc). This fraudulent practice is known as "pro-forma invoicing" and is illegal. People who use this approach often claim to support a charity or worthy community group.

Gambling and Prize Draw Scams

There are countless gambling scams on the Internet. For instance, some Internet sports or casino gambling services require that an individual purchase software - often at a cost of several thousand dollars - that supposedly enable an individual to predict the outcome of horse races or lotteries. However, it is not possible to predict the outcome of random events such as horse races with any certainty. Betting software is often **marketed by showing what an individual would** have made **had** they invested money in the previous year. Here, it is easy for the fraudster to demonstrate that a lot of **money could** have been made when they know which horse won every race. A variety of overseas lottery tickets are also marketed and sold by direct mail in many countries. Very few are legal and fraud is often involved.

Prize scams are extremely popular with fraudsters. Anyone reading such a scam is promised a fabulous prize that they are guaranteed to have won. All an **individual** has **to** do **to claim** the prize is pay a small administration fee - **which** they never see again. They don't get the prize either. Other prize scams include the use of pop-up windows with congratulatory messages such as 'Well done! You're today's Internet winner. Dial [telephone **number] to claim your award** of a holiday/television/car!!!' The pop-up is basically an advertisement as the 'prize' is usually a worthless discount voucher or similar.

Miscellaneous Mail Order Scams

There are many different types of mail order scams **that appear** online. For instance:

Health offers - Consumers are lured into buying vitamins, treatments, or "cures" with the promise of better **health,** fitness or appearance. However, many of the products and treatments being promoted are not regulated by the FDA **and** may be ineffective or harmful.

Fraudulent degrees - Scam artists fronting fictitious schools offer diplomas in exchange for cash. The diplomas look **like** official degrees from prestige-sounding universities, but are actually worthless.

As has been shown, the Internet medium is generating is providing a new medium for criminals and fraudsters to prosper.

Reference

Griffiths, M.D. (2003) "Exploitation and Fraud on the **Internet: Some Common** Practices". *The Criminal Lawyer* 132,5-7.

Professor Mark Griffiths, Psychology Division, Nottingham Trent University.